

associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server.

6. The method of claim 5 further comprising:
storing the client authorization credential at the
first server;
generating a single-use service token associated
5 with the client or the user of the client; and
sending to the client the single-use service token
along with the response and the single-use domain token.

7. The method of claim 1 further comprising:
10 receiving a login request from the client at the
second server;
challenging the client to provide authentication
data;
receiving authentication data from the client;
15 authenticating the client;
generating a single-use domain token associated with
the client or the user of the client;
generating an authentication response; and
sending the authentication response and the
20 single-use domain token to the client.

8. The method of claim 7 further comprising:
determining that the login request is a redirected
request from the first server; and
25 modifying the authentication response to redirect
the client to the first server.

FOUOESD" 35796860

9. An apparatus for controlling access to protected resources within a distributed data processing system, the apparatus comprising:

5 means for receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

means for validating the single-use token, wherein the single-use token comprises session information for performing session management with respect to the client;

means for generating a response to the request;

means for refreshing the single-use token; and

means for sending the response and the refreshed single-use token to the client.

10. The apparatus of claim 9 further comprising:

means for determining that the single-use token is a service token, wherein a service token is issued by the first server; and

20 means for refreshing the single-use service token at the first server.

11. The apparatus of claim 9 wherein the session information in the single-use token is a session key.

25

1002990" 56T 96660

means for sending to the first server the client
25 authorization credential, the refreshed single-use domain
token associated with the client or the user of the
client, and the refreshed single-use domain token
associated with the first server.

credential at the first server;

means for sending to the client the single-use service token along with the response and the single-use domain token.

means for receiving a login request from the client
at the second server;

```

means for challenging the client to provide
authentication data;

```

```
15         means for receiving authentication data from the
        client;
```

means for authenticating the client;

means for generating a single-use domain token
associated with the client or the user of the client;

20 means for generating an authentication response; and

means for sending the authentication response and the single-use domain token to the client.

16. The apparatus of claim 15 further comprising:

25 means for determining that the login request is a
redirected request from the first server; and

means for modifying the authentication response to redirect the client to the first server.

instructions for receiving at a first server from a client a request to access a protected resource and a single-use token associated with the client or a user of the client;

```
instructions for generating a response to the
request;
```

instructions for sending the response and the refreshed single-use token to the client.

instructions for determining that the single-use token is a service token, wherein a service token is issued by the first server; and

19. The computer program product of claim 17 wherein the session information in the single-use token is a session key.

```
5      instructions for generating a client authorization
      credential request;
```

21. The computer program product of claim 20 further comprising:

instructions for validating at the second server the single-use domain token associated with the client or the user of the client and the single-use domain token associated with the first server;

```

20         instructions for generating the client authorization
        credential;

```

instructions for refreshing at the second server the
single-use domain token associated with the client or the
user of the client and the single-use domain token
associated with the first server; and

instructions for sending to the first server the client authorization credential, the refreshed single-use domain token associated with the client or the user of the client, and the refreshed single-use domain token associated with the first server.

5 instructions for generating a single-use service
token associated with the client or the user of the
client; and

10

15

20

```

        instructions for generating a single-use domain
token associated with the client or the user of the
client;

```

25

instructions for sending the authentication response and the single-use domain token to the client.

24. The computer program product of claim 23 further comprising:

instructions for determining that the login request is a redirected request from the first server; and

5 instructions for modifying the authentication response to redirect the client to the first server.

0996195-063001
FOIE90-2578880